module to detect network content. In the illustrated embodiments, filtering module 112 is configured to operate with CPRL module 114, hard coded signature module 116, and heuristics module 118. If no matches are found by filtering module 112, the network content or file stream is then passed to CPRL module 114, hard coded signature module 116, and heuristics module 118.

[0024] CPRL module 114 applies CPRL signatures to the network content to determine if any of the CPRL signatures matches with the network content. Like predicate logic, a signature codified using CPRL is treated as a formula made up of logical elements and is rule-based. Unlike traditional virus signatures, which are used to detect virus using byte-by-byte comparison, a signature created using CPRL represents one or more instructions that control an operation of a processor being used to detect content. For examples, a signature created using CPRL may provide instructions for calling functions, pointing to a different signature, calling an interpreter of the signature recursively, responding to a returned information, and/or performing other functions. As such, CPRL is a true pattern recognition language, and is far more powerful then traditional antivirus signatures. CPRL language, and systems and methods of using CPRL language, have been described in U.S. Patent Application Serial Nos. 10/624,914; 10/624,452; 10/624,941; 10/624,948, all filed on July 21, 2003, the disclosures of which are expressly incorporated by reference herein. In alternative embodiments, instead of using CPRL module 114, binary scanning module 108 can include other types of detection devices or content processors to process network content that has